

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

CORNELIUS COLEMAN AND LINDA HORAN, *on  
behalf of themselves and all others similarly situated*,

v.

RAILWORKS CORPORATION, KEVIN RIDDETT  
AND BOB CUMMINGS,

*Defendants.*

*Plaintiffs,*

CLASS ACTION COMPLAINT  
AND DEMAND FOR JURY TRIAL

Civil Action Number  
1:20-cv-02428

Plaintiffs Cornelius Coleman and Linda Horan (collectively, “Named Plaintiffs”), individually and on behalf of other persons similarly situated (collectively “Plaintiffs” or the “Class”), by and through their attorneys, Thomas & Solomon LLP, bring this class action complaint against RailWorks Corporation, Kevin Riddett and Bob Cummings (“RailWorks” or “Defendants”), and allege as follows:

**NATURE OF ACTION**

1. Named Plaintiffs and other Class Members are all persons, whether current or former employees or otherwise, whose personally identifiable information (“PII”) was compromised as a result of the Data Breach that occurred in or around the beginning of 2020 (“Data Breach” or “Breach”). Defendants betrayed Plaintiffs’ trust by failing to properly safeguard and protect their PII and by disclosing their PII to cybercriminals.

2. This lawsuit seeks to redress RailWorks’ unlawful disclosure of the PII of all persons, regardless of whether they were current and former employees of Defendants, in a massive data breach in or around the beginning of 2020.

3. The Breach occurred as a result of a cyberattack, which resulted in the disclosure of Plaintiffs’ PII, including but not limited to their: name, address, driver’s license number

and/or government issued ID, Social Security number, date of birth and date of hire/termination and/or retirement. The Breach affected numerous persons, some examples being current and former employees of Defendants, including their family members, and current former independent contractors of Defendants, including their family members, and others.

4. For the rest of their lives, Plaintiffs will bear an immediate and heightened risk of all manners of identity theft. Accordingly, Named Plaintiffs bring this action as a direct and/or proximate result of the Data Breach. Plaintiffs have incurred and will continue to incur damages in the form of, *inter alia*, attempted identity theft, time and expenses mitigating harms, increased risk of harm, diminished value of PII, loss of privacy, and/or additional damages set forth below.

#### JURISDICTION AND VENUE

5. The jurisdiction of this Court is invoked pursuant to Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(d)(2), because there are at least 100 class members, the amount in controversy exceeds five million, and there is minimal diversity of citizenship.

6. This Court has personal jurisdiction over RailWorks Corporation because RailWorks maintains its principal place of business in this District, is registered to conduct business in New York, and has sufficient minimum contacts with New York.

7. This Court has personal jurisdiction over the individual defendants, Messrs. Riddett and Cummings, because they are believed and therefore averred to work in New York at RailWorks' headquarters, and have had sufficient minimum contacts with New York.

8. Venue is appropriate in the Southern District of New York because RailWorks resides in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

### **THE PARTIES**

#### ***Named Plaintiffs***

9. Named Plaintiff Cornelius Coleman is a former employee of RailWorks.

10. Mr. Coleman provided his confidential information along with the confidential information of his spouse and two minor children in connection with his employment.

11. Mr. Coleman, his spouse, and his two minor children each received a notice dated on or about February 27, 2020 from RailWorks informing them that RailWorks had disclosed their PII in the Data Breach.

12. Mr. Coleman, his spouse, and his two minor children reasonably expected that RailWorks would maintain the privacy of their confidential PII.

13. Named Plaintiff Linda Horan is a former employee of RailWorks.

14. Ms. Horan provided her confidential information along with the confidential information of her spouse and three children in connection with her employment.

15. Ms. Horan, her spouse, and three children each received a notice dated on or about February 27, 2020 from RailWorks informing them that RailWorks had disclosed their PII in the Data Breach.

16. Ms. Horan, her spouse, and three children reasonably expected that RailWorks would maintain the privacy of their confidential PII.

***Defendants***

17. RailWorks is a Delaware corporation with its principal place of business at 5 Penn Plaza, 15th Floor, New York, New York.

18. Kevin Riddett is the president and CEO of RailWorks. As the president and CEO of RailWorks, Mr. Riddett was responsible for ensuring that RailWorks, including its Chief Information Officer (“CIO”) Mr. Cummings, implemented appropriate cybersecurity to protect the PII of Plaintiffs.

19. Bob Cummings is the CIO of RailWorks. As the senior officer responsible for all information technology and systems functions for RailWorks and its subsidiaries, Mr. Cummings was responsible for protecting the PII of Plaintiffs.

**FACTS**

20. On or about January 27, 2020, an unauthorized third party encrypted Defendants’ servers and systems resulting in the Data Breach and exposure of the PII of thousands of persons.

21. Some Plaintiffs received an email notification on or about January 30, 2020 and/or February 7, 2020, from Defendants informing them of the Breach. Other Plaintiffs received or should have received correspondence at varying points throughout March 2020, and dated on or about February 27, 2020, informing them of the breach. Therefore, Defendants did not inform some of the Plaintiffs for over a month following the Breach.

22. The correspondence received by Plaintiffs informed them that as a result of the Breach, their PII was compromised, which could include their name, address, driver’s license number and/or government issued ID, Social Security number, date of birth and date of hire/termination and/or retirement.

23. By disclosing Plaintiffs' PII to cybercriminals, Defendants put all Plaintiffs at risk.

24. Defendants negligently failed to take the necessary precautions required to safeguard and protect Plaintiffs' PII from unauthorized disclosure. Defendants' actions and/or inactions represent a flagrant disregard of Plaintiffs' rights, both as to privacy and property.

***Personally Identifiable Information (PII)***

25. PII is of great value to hackers and cyber criminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners.

26. The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. along, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." *See* Office of Mgmt & Budget, OMB Memorandum M-07-16 n.1, available at <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf>.

27. Given the nature of this Breach, it is foreseeable that cybercriminals can and will use the compromised PII in a variety of different ways.

***Defendants Were Aware of the Risk Of Cyberattacks***

28. Data security breaches are becoming increasingly more prevalent. In fact, in the wake of the rise in data breaches, the Federal Trade Commission has issued an abundance of guidance for companies. *See e.g., Protecting Personal Information: A Guide for Business*, FTC, available at <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>.

29. Further, data breach issues had been at record number in 2019. According to statistics from nortom.com, there was a 54% increase in publicly reported data breaches in the first six months of 2019 versus the first six months of 2018. See *2019 Data Breaches: 4 Billion Records Breached so Far*, Norton, available at <https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html>.

30. Therefore, Defendants clearly knew or should have known of the risks of data breaches and thus should have ensured that the adequate protections were in place.

***Plaintiffs Have Suffered Concrete Injuries***

31. Plaintiffs were obligated to provide Defendants with sensitive personal information.

32. The Class Members are at an increased risk that the cybercriminals will use their PII for the rest of their lives, and in some cases the cybercriminals have already used such PII to steal Class Members' identities. Plaintiffs bring this action because as a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs have incurred and will continue to incur damages in the form of, *inter alia*, attempted identity theft, time and expenses mitigating harms (e.g., the costs of engaging credit monitoring and protection services), increased risk of harm, diminished value of PII, and/or loss of privacy. By this action, Plaintiffs seek to hold Defendants responsible for the harm caused by its negligence.

33. In addition, as a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs have been deprived of the value of their PII, for which there is a well-established national and international market.

34. Defendants' wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported.

35. Certain Plaintiffs have already been victim to fraudulent activity since the occurrence of the Breach. For example, Named Plaintiff Linda Horan and one of her children have both been victim to fraudulent activity on their respective personal credit cards.

***Defendants Response To The Data Breach Is Inadequate To Protect The Plaintiffs***

36. Defendants have failed to provide adequate compensation to the Plaintiffs harmed by their negligence. To date, Defendants have offered Plaintiffs just twelve (12) months of credit monitoring through Identity Guard Total service. Even if a Plaintiff signs up for Identity Guard Total, it will not provide Plaintiffs any compensation for the costs and burdens associated with fraudulent activity resulting from the Data Breach that took place prior to a Plaintiff signing up. This is especially concerning where some Plaintiffs were not informed that their PII was compromised until over a month following the Breach.

37. Additionally, Identity Guard Total does nothing to protect *against* identity theft. Instead, it only provides various measures to detect identity theft once it has already been committed. For example, Identity Guard Total "monitors and process billions of pieces of information to alert [employees] about threats to [their] identity."

38. In addition, Plaintiffs have reported major difficulties getting through to the call center Defendants referred them to regarding any questions they may have, denying them the ability to promptly gather the necessary information to protect themselves. In fact, when Named Plaintiff Linda Horan emailed RailWorks' Sr. Vice President, Human Resources

regarding her inability to get through to the call center, he merely responded stating, “[y]es, the telephone number and messages are being taken care of by a 3rd party for us. They are aware of the issue and are having it fixed. Give it a couple days before going into it again.” This response again shows a complete disregard for the severity of the matter and a lack of urgency to ensure that those effected obtained the necessary protections in a timely manner.

39. Further, Defendants through the third party call center and/or generally, have repeatedly failed to provide adequate responses to Plaintiffs questions and concerns. For example, when Plaintiffs asked representatives through the call center regarding whether the credit monitoring service being offered applied retroactively from the date of the Breach, they were either merely not given an answer, referred back to RailWorks, or in some cases even hung up on.

#### **CLASS ACTION ALLEGATIONS**

40. Pursuant to Federal Rule of Civil Procedure 23 (“Rule 23”) Named Plaintiffs bring this action against Defendants as a class action on behalf of themselves and all members of the class of similarly situated persons (“Class”):

All persons, whether current and former employees or otherwise, whose PII was compromised as a result of the Data Breach that occurred in or around the beginning of 2020.

41. Defendants are liable to the Class under the statutes, laws, and regulations of each state in which they operate, including but not limited to: New York; Massachusetts; New Jersey; Maryland; Florida; Georgia; Missouri; Indiana; Illinois; Wisconsin; Minnesota; Nebraska; Louisiana; Texas; California; Utah; and Washington.

42. This includes all causes of action that are designed to prevent companies from allowing the improper disclosure of PII, including but is not limited to:

- N.Y. Gen. bus. Law § 899-aa
- Cal. Bus. & Prof. Code § 17200 *et seq.*
- Cal. Civil Code §§ 56.06, 1785.11.2, 1797.29, 1798.80, 1798.81.5, 1798.82, 1798.84
- Mass. Gen. Laws ch. 93A § 9, ch. 93H
- Tex. Bus. & Com. Code Ann. § 521.052
- Wash. Rev. Code § 19.255.020
- Utah Code §§ 13-44-101, 102, 202, 301
- La. Rev. Stat. Ann. § 51:3071 *et seq.*
- Neb. Rev. Stat. §§ 87-801 – 87-807
- Minn. Stat. §§ 325E.61, 325E.64
- Wis. Stat. § 895.507
- 815 ILCS 530/1 *et seq.*
- Ind. Code §§ 24-4.0 *et seq.*, 4-1-11 *et seq.*
- Ga. Code §§ 10-1-910, 912
- Fla. Stat. § 817.5681
- Md. Code Com. Law § 14-3501
- N.J. Stat. 56:8-163

43. Plaintiffs reserve the right to amend the above definition(s), or to propose other or additional classes, in subsequent pleadings and/or motions for class certification.

44. The class action is maintainable under subsections (1), (2), (3) and (4) of Rule 23(a).

45. Plaintiffs believe that the proposed Class consists of thousands of members. Thus, the Class is so numerous that joinder of all members is impracticable.

46. Common issues of law and fact exist as to all members of the Class and predominate over any questions affecting only individual class members. Among the common issues of law and fact are the following:

- Whether and to what extent Defendants had a duty to protect the Class Members' PII;
- Whether Defendants breached their duty to protect the Class Members' PII;
- Whether the actions and/or inaction of Defendants caused the Class Members' PII to be compromised;
- Whether Defendants disclosed Class Members' PII;

- Whether Defendants conduct was negligent; and
- Whether Defendants are liable for all damages claimed.

47. The Named Plaintiffs' claims are typical of the claims of other members of the Class because, *inter alia*, Named Plaintiffs' and Class Members sustained similar injuries as a result of Defendants' uniform wrongful conduct; Defendants owed the same duty to each Class Member; and Class Members' legal claims arise from the same conduct by Defendants.

48. Named Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Named Plaintiffs have no interest antagonistic to the Class, and have retained counsel experienced in class action litigation.

49. Class counsel Thomas & Solomon LLP is qualified and able to litigate Named Plaintiff and Class claims.

50. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and avoids duplication by allowing these claims to be prosecuted in a single action. Named Plaintiffs and members of the Class lack the resources to adequately prosecute separate claims, and the amount that each individual stands to recover makes individual cases impractical to pursue.

51. The class action is maintainable under subsection (1) of Rule 23(b) because the prosecution of separate actions by individual Class Members would create a risk of establishing incompatible standards of conduct for Defendants.

52. The class action is also maintainable under subsection (2) of Rule 23(b) because Defendants' acted, or refused to act, on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or equitable relief with respect to the Class as a whole.

53. Moreover, the class is maintainable under subsection (3) of Rule 23(b) because the above common questions of law or fact predominate over any questions affecting individual Class Members and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

**FIRST CAUSE OF ACTION**  
*Negligence*

54. Plaintiffs hereby re-allege the above paragraphs as if fully restated herein.

55. As a condition of their employment, Employees and Independent Contractors were obligated to provide Defendants with certain of their and in some cases their immediate family members' PII.

56. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs could and would suffer if the PII were compromised. Defendants had a duty to Plaintiffs to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiffs were the foreseeable victims of any inadequate safety and security practices. Plaintiffs had no ability to protect their data that was in Defendants' possession.

57. Defendants had a duty to Plaintiffs to safeguard and protect their PII. Defendants' duty to Plaintiffs included, *inter alia*, establishing processes and procedures to protect the PII from wrongful disclosure and to ensure that proper cyber-security measures were in place.

58. Defendants assumed a duty of care to use reasonable means to secure and safeguard this PII, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of its servers and systems.

59. Defendants had a duty to use ordinary care in activities from which harm might be reasonably anticipated in connection with Plaintiffs' PII data.

60. Defendants breached its duty of care by failing to secure and safeguard the PII of Plaintiffs. Defendants negligently stored and/or maintained its servers and systems.

61. Plaintiffs have suffered harm as a result of Defendants' negligence. These victims' loss of control over the compromised PII subjects each of them to a greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from the use of the compromised information.

62. It was reasonable foreseeable in that Defendants knew or should have known that its failure to exercise adequate care in safeguarding and protecting Plaintiffs' PII would result in its release and disclosure to unauthorized third parties who, in turn, wrongfully used such PII or disseminated it to other fraudsters for their wrongful use and for no lawful purpose.

63. But for Defendants' negligent and wrongful breach of its responsibilities and duties owed to Plaintiffs, their PII would not have been compromised.

64. As a direct and proximate result of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' PII, Plaintiffs have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm – for which they are entitled to compensation. Defendants' wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

65. Plaintiffs are entitled to injunctive relief as well as actual and punitive damages.

**SECOND CAUSE OF ACTION**

***Breach of Express Contract***

66. Plaintiffs hereby re-allege the above paragraphs as if fully restated herein.

67. Plaintiffs or their immediate family members had written employment agreements with Defendants. The employment agreements involved a mutual exchange of

consideration whereby Defendants entrusted Plaintiffs with particular job duties and responsibilities in furtherance of RailWorks services, in exchange for the promise of employment, with salary, benefits, and secure PII.

68. Defendants' failure to protect Plaintiffs' PII constitutes a material breach of the terms of the agreement by Defendants.

69. As a direct and proximate result of Defendants' breach of contract with Plaintiffs, Plaintiffs have been irreparably harmed.

70. Accordingly, Plaintiffs respectfully request this Court award all relevant damages for Defendants' breach of express contract.

**THIRD CAUSE OF ACTION**  
***Breach of Implied Contract***

71. Plaintiffs hereby re-allege the above paragraphs as if fully restated herein.

72. Defendants required Plaintiffs to furnish their PII, which included, *inter alia*, names, addresses, driver's license numbers and/or government issued IDs, Social Security numbers, dates of birth, as a condition precedent of their employment. Defendants required the sensitive information to verify their identities, provide agreed-upon compensation and benefits, and for tax purposes, amongst other things.

73. Understanding the sensitive nature of the PII, Defendants implicitly promised Plaintiffs that it would take adequate measure to protect their PII.

74. Plaintiffs reasonably relied upon this covenant and would not have disclosed their PII without assurances that it would be properly safeguarded.

75. Plaintiffs fulfilled their obligations under the contract by providing their PII to Defendants, and by upholding their obligations.

76. As the direct and proximate result of Defendants' breach of the contract between Defendants and Plaintiffs, Plaintiffs sustained actual losses and damages as described above.

77. Accordingly, Plaintiffs respectfully request this Court award all relevant damages for Defendants' breach of implied contract.

**FOURTH CAUSE OF ACTION**  
*Unjust Enrichment*

78. Plaintiffs hereby re-allege the above paragraphs as if fully restated herein.

79. Defendants, by way of its affirmative actions and omissions, knowingly and deliberately enriched itself by saving the costs it reasonably and contractually should have expended on data security measures to secure Plaintiffs' PII.

80. Nevertheless, Defendants continued to obtain the benefits conferred on it by Plaintiffs or Plaintiffs' immediate family members employment, mainly from the labor contracted to in the employment agreements between the parties.

81. As a direct and proximate result of Defendants' decision to profit rather than provide adequate security, and Defendants' resultant disclosures of Plaintiffs' PII, Plaintiffs suffered and continue to suffer considerable injuries in the forms of attempted identity theft, time and expenses mitigating harms, diminished value of PII, loss of privacy, and increased risk of harm.

82. Accordingly, Plaintiffs respectfully request this Court award relief in the form of restitution and/or compensatory damages.

**FIFTH CAUSE OF ACTION**  
*N.Y. Labor Law § 203-d*

83. Plaintiffs hereby re-allege the above paragraphs as if fully restated herein.

84. Pursuant to New York law, “[a]n employer shall not unless otherwise required by law: . . . (c) Place a social security number in files with unrestricted access; or (d) Communicate an employee’s personal identifying information to the general public.” N.Y LABOR LAW § 203-d(1).

85. “[P]ersonal identifying information” is defined as including an individual’s “social security number, home address or telephone number, personal electronic mail address, Internet identification name or password, parent’s surname prior to marriage, or drivers’ license number.” N.Y LABOR LAW § 203-d(1)(d).

86. The statute further mandates that “[i]t shall be presumptive evidence that a violation of this section was knowing if the employer has not put in place any policies or procedures to safeguard against such violation, including procedures to notify relevant employees of these provisions.” N.Y LABOR LAW § 203-d(3).

87. Defendants’ acts and omission were unlawful in violations of N.Y LABOR LAW § 203-d because Defendants had not put into place policies, procedures or sufficient safeguards against such violations, as made evident by Defendants susceptibility to cyberattacks.

88. Accordingly, Plaintiffs respectfully request this Court award statutory damages, compensatory damages, and injunctive relief for Defendants’ violation of N.Y LABOR LAW § 203-d.

**SIXTH CAUSE OF ACTION**  
***Violation of the Applicable State Laws***

89. Plaintiffs hereby re-allege the above paragraphs as if fully restated herein.

90. As a direct and proximate result of Defendants’ above-described wrongful actions, inactions, and omissions, resulting in the improper disclosure of Plaintiffs’ PII,

Defendants' are in violation of the following and other similar state laws designed to protect Plaintiffs' from the unauthorized disclosure of their PII:

- N.Y. Gen. bus. Law § 899-aa
- Cal. Bus. & Prof. Code § 17200 *et seq.*
- Cal. Civil Code §§ 56.06, 1785.11.2, 1797.29, 1798.80, 1798.81.5, 1798.82, 1798.84
- Mass. Gen. Laws ch. 93A § 9, ch. 93H
- Tex. Bus. & Com. Code Ann. § 521.052
- Wash. Rev. Code § 19.255.020
- Utah Code §§ 13-44-101, 102, 202, 301
- La. Rev. Stat. Ann. § 51:3071 *et seq.*
- Neb. Rev. Stat. §§ 87-801 – 87-807
- Minn. Stat. §§ 325E.61, 325E.64
- Wis. Stat. § 895.507
- 815 ILCS 530/1 *et seq.*
- Ind. Code §§ 24-4.0 *et seq.*, 4-1-11 *et seq.*
- Ga. Code §§ 10-1-910, 912
- Fla. Stat. § 817.5681
- Md. Code Com. Law § 14-3501
- N.J. Stat. 56:8-163

91. Accordingly, Plaintiffs respectfully request the appropriate relief available under each of the state laws.

**WHEREFORE**, Named Plaintiffs and Class Members demand judgment against Defendants in their favor and that they be given the following relief:

- a. appropriate injunctive relief and/or declaratory relief, including an Order requiring Defendants to properly secure and fully encrypt all confidential information, to cease negligently storing, handling, and securing confidential information, and to provide lifetime credit monitoring and identity theft repair services;
- b. an award of appropriate compensatory, statutory, and general damages;
- c. an award of reimbursement, restitution, and disgorgement;
- d. an order certifying the class as requested and designating Thomas & Solomon LLP as class counsel;
- e. designation of Named Plaintiffs Cornelius Coleman and Linda Horan as class representatives;

- f. an award of reasonable attorneys' fees, expenses, expert fees and costs incurred in vindicating Named Plaintiffs' and Class Members' rights;
- g. an award of pre- and post-judgment interest;
- h. service payments for the Named Plaintiffs; and
- i. such other and further legal or equitable relief as this Court deems to be just and appropriate.

**JURY DEMAND**

Plaintiffs demand a jury to hear and decide all issues of fact in accordance with Federal Rule of Civil Procedure 38(b).

Dated: March 19, 2020

THOMAS & SOLOMON LLP

By:



J. Nelson Thomas, Esq.

Jessica L. Lukasiewicz, Esq.

*Attorneys for Plaintiffs*

693 East Avenue

Rochester, New York 14607

Telephone: (585) 272-0540

[nthomas@theemploymentattorneys.com](mailto:nthomas@theemploymentattorneys.com)

[jlukasicewicz@theemploymentattorneys.com](mailto:jlukasicewicz@theemploymentattorneys.com)